Ataques a la Tríada CIA (Confidencialidad, Integridad y Disponibilidad)

Carrera: Tecnologías de la Información y Telecomunicaciones
Materia_ID: SEC_NET_01
Materia: Seguridad en Redes y Tecnología de la Información I

Título del Trabajo: Ataques a la Tríada CIA (Confidencialidad, Integridad y Disponibilidad)

Alumno
Ing. Jorge Parra Hidalgo
ID: 13104

Docente
MSI. Raúl Alberto Toledo Piñón

Tabla de contenido

Introducción

La seguridad de la información es un pilar fundamental en la actualidad, especialmente ante el crecimiento del uso de sistemas informáticos, redes y servicios digitales. Para proteger la información, se utiliza el modelo de la Tríada CIA, que representa los principios de Confidencialidad, Integridad y Disponibilidad. Estos principios buscan garantizar que la información solo sea accesible por usuarios

autorizados, que no sea alterada sin permiso y que esté disponible cuando se necesite.

Sin embargo, existen múltiples técnicas y métodos de ataque que buscan vulnerar alguno o varios de estos principios. Dichos ataques pueden ser tecnológicos, humanos o incluso físicos, y representan un riesgo constante para organizaciones y usuarios. En esta investigación se analizan diversas formas de ataque a la Tríada CIA, explicando su funcionamiento, el principio de seguridad que afectan y su impacto potencial en los sistemas de información.

Desarrollo

2.1 Packet Sniffing

El packet sniffing es una técnica que consiste en la captura y análisis de paquetes de datos que circulan a través de una red. Los atacantes utilizan herramientas especializadas para interceptar información como contraseñas, correos electrónicos o datos personales.

Este ataque afecta principalmente la confidencialidad, ya que permite acceder a información sensible sin autorización. Es común en redes mal configuradas o sin cifrado, como redes Wi-Fi públicas.

2.2 Password Cracking

El password cracking consiste en obtener contraseñas mediante técnicas como fuerza bruta, diccionario o ataques híbridos. El objetivo es acceder de manera no autorizada a sistemas, cuentas o servicios.

Este tipo de ataque compromete la confidencialidad y, en algunos casos, la integridad, ya que el atacante puede modificar información una vez que obtiene acceso.

2.3 Dumpster Diving

El dumpster diving es una técnica no tecnológica que consiste en buscar información sensible en la basura, como documentos impresos, discos duros o dispositivos USB desechados.

Afecta directamente la confidencialidad, demostrando que la seguridad de la información no solo depende de sistemas digitales, sino también de prácticas físicas y administrativas.

2.4 Wiretapping

El wiretapping implica la interceptación de comunicaciones, ya sea telefónicas o de red, sin el consentimiento de los participantes. Puede realizarse de forma física o digital.

Este ataque vulnera la confidencialidad de la información transmitida.

2.5 Keylogging

El keylogging es una técnica que registra las pulsaciones del teclado de un usuario para obtener contraseñas, mensajes u otra información confidencial. Puede ser implementado mediante software o hardware.

Compromete principalmente la confidencialidad y puede derivar en ataques adicionales.

2.6 Phishing

El phishing es un ataque de ingeniería social en el que el atacante engaña al usuario para que proporcione información sensible, haciéndose pasar por una entidad legítima.

Afecta la confidencialidad y puede provocar pérdidas económicas o robo de identidad.

2.7 Ataque Salami

El ataque salami consiste en realizar pequeños cambios o robos de información o dinero que pasan desapercibidos individualmente, pero que en conjunto generan un impacto significativo.

Este ataque afecta la integridad de los datos y sistemas.

2.8 Data Diddling

El data diddling implica la modificación de datos antes o durante su procesamiento, alterando resultados finales sin ser detectado fácilmente.

Compromete la integridad de la información.

2.9 Session Hijacking

El session hijacking ocurre cuando un atacante toma control de una sesión activa entre un usuario y un sistema, generalmente robando cookies de sesión.

Afecta la confidencialidad y la integridad.

2.10 Man-in-the-Middle

En un ataque man-in-the-middle, el atacante se coloca entre dos partes que se comunican, interceptando y alterando la información transmitida.

Este ataque vulnera tanto la confidencialidad como la integridad.

2.11 DoS y DDoS

Los ataques de Denegación de Servicio (DoS) y Denegación de Servicio Distribuida (DDoS) buscan saturar un sistema o red para que no pueda ofrecer sus servicios.

Afectan directamente la disponibilidad.

2.12 SYN Flood

El SYN flood es un tipo específico de ataque DoS que explota el proceso de establecimiento de conexiones TCP enviando múltiples solicitudes incompletas.

Compromete la disponibilidad del sistema.

2.13 Ataques físicos a la infraestructura de servidores

Estos ataques incluyen el robo, daño o sabotaje de servidores, cables, centros de datos o sistemas de energía.

Pueden afectar la confidencialidad, integridad y disponibilidad de la información.

Conclusiones

Los ataques a la Tríada CIA representan una amenaza constante para la seguridad de la información en cualquier organización. A lo largo de esta investigación se analizó cómo distintos tipos de ataques pueden comprometer la confidencialidad, integridad y disponibilidad de los sistemas, ya sea mediante técnicas tecnológicas avanzadas, ingeniería social o ataques físicos.

Es evidente que la seguridad informática no depende únicamente de herramientas tecnológicas, sino también de la concientización de los usuarios, políticas de seguridad adecuadas y buenas prácticas organizacionales. Implementar controles de acceso, cifrado, monitoreo de redes y medidas físicas de protección es fundamental para reducir los riesgos.

Finalmente, comprender estos ataques permite a las organizaciones anticiparse a las amenazas y fortalecer sus estrategias de seguridad, garantizando así la protección de la información y la continuidad de sus operaciones.

Glosario de términos

Confidencialidad: Principio que garantiza que la información solo sea accesible por personas autorizadas.

Integridad: Asegura que la información no sea alterada de manera no autorizada.

Disponibilidad: Garantiza que los sistemas y datos estén accesibles cuando se requieran.

Malware: Software malicioso diseñado para dañar o comprometer sistemas.

Ingeniería social: Técnicas que manipulan a las personas para obtener información confidencial.

Fuentes consultadas

Stallings, W. (2018). Network Security Essentials: Applications and Standards. Pearson.

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.

NIST. (2020). Computer Security Resource Center. National Institute of Standards and Technology.

Cisco Systems. (2022). Introduction to Cybersecurity. Cisco Networking Academy.